CLAIMS

What is claimed is:

1. A method comprising key distribution in a conditional access system, wherein a set of all user nodes which the system can accommodate is a complete set, and a subset is composed of all or part of the user nodes, said key distribution comprising the steps of:

decomposing said subset into at least one secondary subset;

assigning a different user key to each secondary subset, each said user key being transmitted to all users in a corresponding secondary subset;

encrypting an entitlement key by using each said user key so as to generate a cipher text corresponding to each said secondary subset; and

combining said cipher text to generate a media key control block.

2. A method according to claim 1, further comprising the step of transmitting said media key control block to all users in said subset.

3. A method according to claim 1, wherein a video program is encrypted using said entitlement key.

4. A method according to claim 1, wherein a control word is encrypted using said entitlement key, and a video program is encrypted using said control word.

5. A method according to claim 3, wherein the users of each said secondary subset identifies said cipher text of the secondary subset to which a user belongs from said

media key control block, and decrypts said cipher text by using the user key of said user so as to obtain said entitlement key.

6. A method according to claim 1, wherein said media key control block can be transmitted uni-directionally on a broadcast channel.

7. A method according to claim 1, wherein said decomposed secondary subset can be maintained unchanged after the setup of said system.

8. A method according to claim 1, wherein a binary tree algorithm is used to decompose said subset into said at least one secondary subset.

9. A method according to claim 1, wherein a multiple tree algorithm is used to decompose said subset into said at least one secondary subset.

10. An apparatus for key distribution in a conditional access system, wherein a set of all user nodes which the system can accommodate is a complete set, and a subset is composed of all or part of the user nodes, said apparatus comprising:

a decomposing unit for decomposing said subset into at least one secondary subset, and assigning a different user key to each secondary subset, each said user key being transmitted to all users in a corresponding secondary subset;

a generating unit for encrypting an entitlement key by using each said user key so as to generate each cipher text corresponding to each said secondary subset;

a combining unit for combining said cipher text to generate a media key control block; and an entitlement control means for controlling the corresponding operation of each said unit and outputting said media key control block.

11. An apparatus for key distribution according to claim 10, further comprising a transmitting means for transmitting said media key control block received from said entitlement control means to all users in said subset.

12. A transmitting apparatus in a conditional access system, wherein a set of all user nodes which the system can accommodate is a complete set, and a subset is composed of all or part of the user nodes, comprising:

a decomposing unit for decomposing said subset into at least one secondary subset, and assigning a different user key to each secondary subset, each said user key being transmitted to all users in a corresponding secondary subset;

a generating unit for encrypting an entitlement key using each said user key so as to generate a cipher text corresponding to each said secondary subset;

a combining unit for combining said cipher text to generate a media key control block;

a program scrambling unit for scrambling a video program by using said entitlement key;

a transmitting unit for transmitting the scrambled video program and said media key control block to a receiving apparatus; and

an entitlement control means for controlling the corresponding operation of each of said units and outputting said media key control block to said transmitting unit.

13. A transmitting apparatus according to claim 12, wherein said transmitting apparatus further comprises a control word encrypting unit for encrypting a control word into said

cipher text by using said entitlement key under the control of said entitlement control means, wherein said program scrambling unit encrypts said video program by using said control word.

14. A transmitting apparatus according to claim 13, wherein said cipher text is an entitlement control message (ECM).

15. A transmitting apparatus according to claim 12, wherein said decomposing unit decomposes said subset using a binary tree algorithm into said at least one secondary subset.

16. A transmitting apparatus according to claim 12, wherein said decomposing unit decomposes said subset into said at least one secondary subset using a multiple tree algorithm.

17. A transmitting apparatus according to claim 12, wherein said entitlement control means is also used for controlling user information.

18. A receiving apparatus in a conditional access system, wherein a set of all user nodes which the system can accommodate is a complete set, and a subset is composed of all or part of the user nodes, comprising:

a receiving unit for receiving the scrambled video program and media key control block transmitted from a transmitting apparatus;

a resolving unit for decrypting a cipher text by using a user key so as to obtain an entitlement key, wherein said cipher text is obtained by identifying said media key block using the user key corresponding to the secondary subset to which said receiving apparatus belongs, and said secondary subset is obtained by decomposing said subset; and

a program descrambling unit for decrypting said scrambled video program by using said entitlement key.

19. The receiving apparatus according to claim 18, wherein said receiving apparatus further comprises a control word decrypting unit for decrypting said cipher text by using said entitlement key so as to obtain a control word; wherein said program descrambling unit descrambles said video program by using said control word.

20. The receiving apparatus according to claim 19, wherein said cipher text is an entitlement control message (ECM).

21. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing key distribution, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

22. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for key distribution, said method steps comprising the steps of claim 1.

23. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing key distribution, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 10.

24. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing transmission, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 12.

25. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing reception, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 18.